

Mao Declaration Exhibit A

ADVERTISEMENT

INNOVATION > CYBERSECURITY

Google Confirms It Has Been Hacked — What User Data Has Been Stolen?

By **Davey Winder**, Senior Contributor. ⓘ Davey Winder is a veteran...



Follow Author

Published Aug 09, 2025, 04:43am EDT, Updated Aug 10, 2025, 05:49am EDT

Share Save Comment 2



Google confirms it has been hacked.
SOPA IMAGES/LIGHTROCKET VIA GETTY IMAGES

Update, August 9, 2025: This story, originally published on August 7, has been updated with additional information from cybersecurity experts regarding the now confirmed hacking of Google. This article explores the user data that has been compromised during the attack and what organizations need to do next.

The Google Threat Intelligence Group has officially confirmed that user data has been stolen following a successful hack attack impacting one of its databases. Here's what we know so far.

FORBES

Emergency Microsoft Security Warning Confirmed — Act Now, CISA Says

By Davey Winder



Google Has Been Hacked — Data Has Been Compromised

This is not a warning that the Google Chrome web browser is in need of [an urgent security update](#), or a story about switching from passwords to passkeys to [protect your Google account](#). No, this is exactly what the headline says: Google has been hacked.

Source? That would be Google itself.

An August 5 posting by the Google Threat Intelligence Group has [confirmed](#) that one of the corporate databases was impacted by hackers thought to be associated with the ShinyHunters ransomware group, more formally known as [UNC6040](#).

“Google responded to the activity, performed an impact analysis and began mitigations,” the GTIG posting stated, adding the database in question was a Salesforce instance “used to store contact information and related notes for small and medium businesses.”

MORE FOR YOU

Hulu’s Best New Show Has A Near-Perfect Rotten Tomatoes Score



Powerball Jackpot Rises To \$565 Million—Here’s What The Winner Could Take Home After Taxes



Everything To Know About ‘The Life Of A Showgirl’—Release Date, Tracklist And More



“The speed at which organisations are falling victim to cyber attacks targeting Salesforce instances is nothing short of alarming,” Robin Brattel, CEO at Lab 1, said. “We need to be honest: malicious campaigns are being scaled quicker than ever as hackers are using information that’s already been made public, often from past data breaches, to target organisations.”

Customer data was, Google said, “retrieved by the threat actor,” in the short period of time that the attack window remained open. Although Google has not gone into great detail regarding the attack as of yet, it did confirm that the stolen data consisted of “basic and largely publicly available business information, such as business names and contact details.”

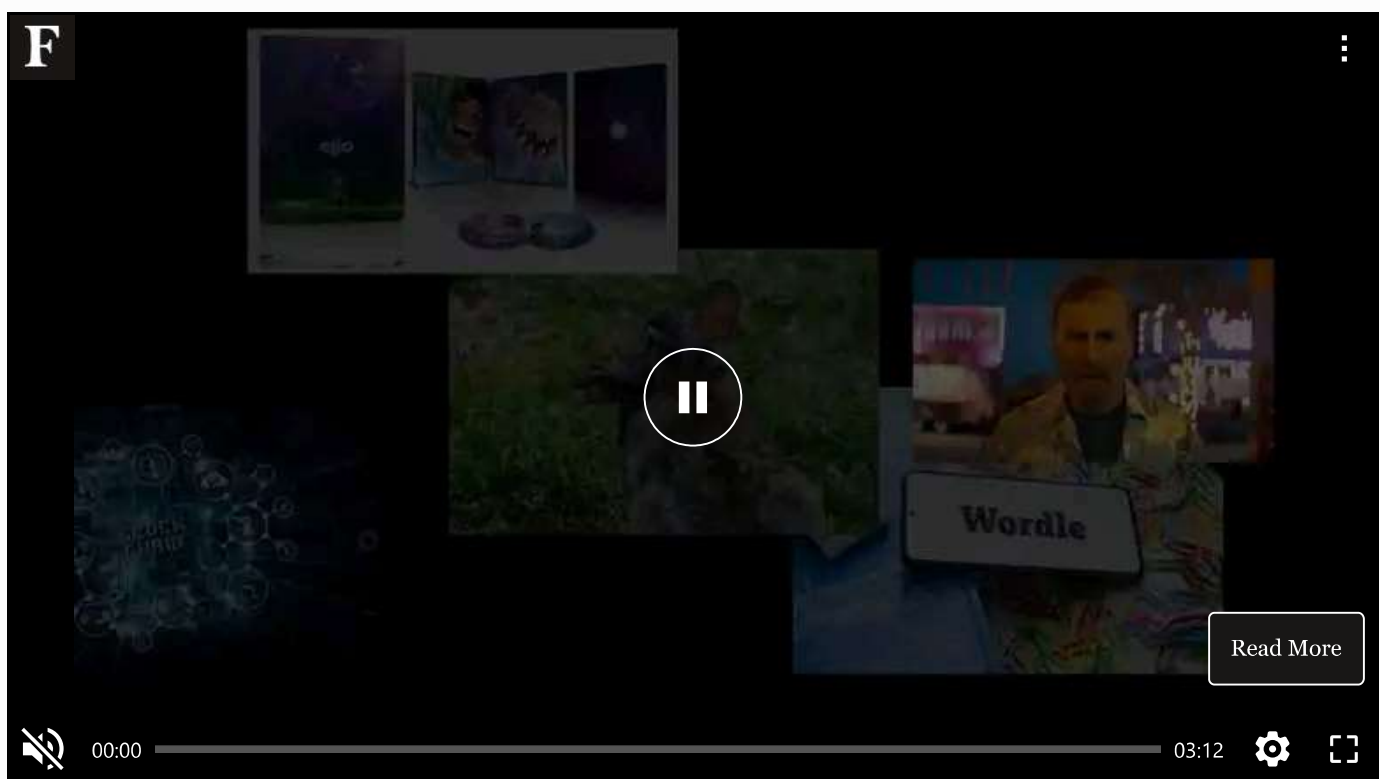
The Prompt: Get the week's biggest AI news on the buzziest companies and boldest breakthroughs, in your inbox.

Email Address

Sign Up

By signing up, you agree to receive this newsletter, other updates about Forbes and its affiliates' offerings, our [Terms of Service](#) (including resolving disputes on an individual basis via arbitration), and you acknowledge our [Privacy Statement](#). Forbes is protected by reCAPTCHA, and the Google [Privacy Policy](#) and [Terms of Service](#) apply.

I reached out to Google for a statement and a spokesperson told me that the “details that we’re able to share at this time can all be found in our blog update,” adding that this includes additional information regarding the ShinyHunters associated UNC6040 threat group, which “provides the security community with actionable intelligence on this actor.”



Google also stated that [ShinyHunters](#) commonly uses an attack tactic of extorting victims using emails or telephone calls demanding bitcoin ransom payments within 72 hours of compromise. It has not, however, confirmed or denied that this was the case here. Google did confirm that the attack itself occurred in June.

FORBES

Microsoft Windows Security Bypass — Hello Hackers Use Own Faces

By Davey Winder



What Cybersecurity Experts Have To Say About The Hacking of Google

“The news that Google has suffered a data breach in the recent wave of attacks executed by ShinyHunters highlights that no organisation is immune to cybercrime,” William Wright, CEO of Closed Door Security, said, adding: “It doesn’t matter if you are a small business or one of the world’s leading technology firms, all organizations are vulnerable.” While Google’s update provides an overview of how these attacks unfolded, Wright continued, “it does not state whether the impacted organisations have been informed, or, if they have been informed, when they were informed.” Which means that the cybercriminals involved, ShinyHunters or not, could have had this information for two months to do with as they saw fit.

“Google has long been one of the leading companies in the world when it comes to cybersecurity,” Jamie Akhtar, CEO of CyberSmart, said, concluding that “if it can happen to one of the wealthiest and best-defended companies in the world, it can happen to anyone.” Akhtar also issued a cautionary word, considering that the attack is being associated with the ShinyHunters ransomware and extortion cybercrime group. “Given what we know about common ransomware methods, it’s very possible this breach stemmed from social engineering or some form of human error,” Akhtar said, adding that this “illustrates that the best technical defences in the world won’t protect you if a member of staff clicks on something they shouldn’t or is artfully duped by social engineering.”

Meanwhile, Dray Agha, senior manager of security operations at Huntress, drew attention to the critical supply chain risks posed by third-party platforms, agreeing with Akhtar’s note of caution. “Even tech giants aren’t immune, highlighting that businesses must rigorously vet and continuously monitor all vendors with access to their data,” Agha warned. “The reported use of voice phishing by UNC6040 is a stark reminder that human factors remain a commonly targeted attack surface.” Which is why, Agha advised that organizations need to invest in a layered approach to security that includes “advanced security awareness training, as well as strict access controls, especially for cloud platforms holding sensitive customer information.”

Some cybersecurity experts went further, insisting that “hacks like this are preventable - in fact, they’re impossible - when enterprises deploy truly credential-less authentication.” Of course, Federico Simonetti, the chief technology officer at Xiid, would say that as he has skin in the game, but that doesn’t negate the point being made. If a hacker calls an IT help desk in an attempt to socially engineer their way to a user password reset, Simonetti said, they can’t. “Today, credential-less authentication isn’t just a nice-to-have,” Simonetti insisted, “it’s an essential.”

I’ll leave the final word to Akhtar though, who noted that “while any breach at Google is shocking, there’s no indication as yet that any of the data stolen is particularly sensitive or places customers in real peril.” Indeed, Google has already stated that the compromised user data is a Salesforce instance containing publicly available information. “As such,” Akhtar concluded, “our advice to businesses is to be cautious but don’t panic.”

FORBES

Camera Hacking — America's Cyber Defense Agency Issues Warning

By **Davey Winder**



**CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY**

[Editorial Standards](#)

[Reprints & Permissions](#)



Find [Davey Winder](#) on [LinkedIn](#) and [X](#). Visit [Davey's website](#). Browse [additional work](#).

[Follow Author](#)

Join The Conversation

Comments 2

One Community. Many Voices. Create a free account to share your thoughts. Read our community guidelines [here](#).

[See All Comments \(2\)](#)

RELATED TOPICS

- | | | | |
|-------------------|---|-----------------|---|
| 01. CHECK IF YOUR | > | 05. HOW TO STOP | > |
| 02. HOW TO SCAN | > | 06. 5 CRYPTO | > |
| 03. 10 SIGNS YOUR | > | 07. BEST FREE | > |
| 04. HOW TO CHECK | > | 08. BEST PASSWO | > |

SEE ALSO



Forbes

© 2025 Forbes Media LLC. All Rights Reserved.

[AdChoices](#) [Privacy Statement](#) [✔✕ Your Privacy Choices](#) [Cookie Preferences](#) [Digital Terms of Sale](#) [Terms of Service](#)

[Contact Us](#) [Send Us Feedback](#) [Report a Security Issue](#) [Jobs At Forbes](#) [Reprints & Permissions](#) [Forbes Press Room](#)

[Advertise](#)